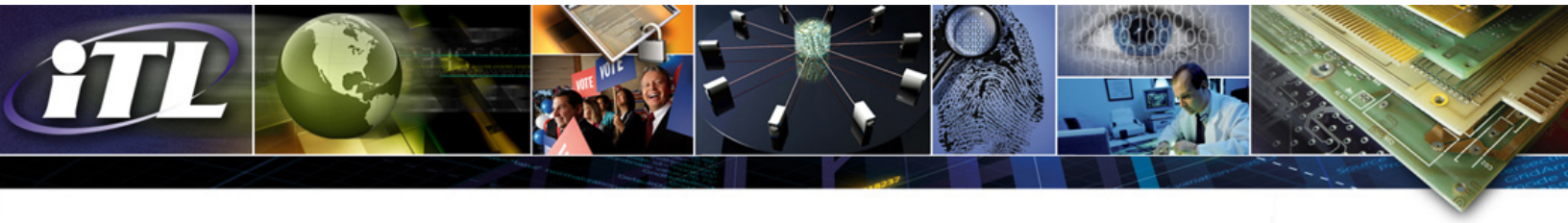

ITL BULLETIN FOR DECEMBER 2014

RELEASE OF NIST SPECIAL PUBLICATION 800-157, *GUIDELINES FOR DERIVED PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS*

Hildegard Ferraiolo, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

Members of the federal government are increasingly using Personal Identity Verification (PIV) cards that uniquely identify the cardholder through verification of electronically stored credentials. PIV smart cards are used to allow the cardholder access to government facilities or to access federal computer systems (e.g., desktops and laptops) equipped with smart card readers. In the last decade, the mobile computing device market has skyrocketed, with a resulting desire by both employers and employees to enable remote access from these devices.

NIST has recently released Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, *to* provide the technical details for a system by which mobile devices such as smart phones and tablets are provisioned with PIV credentials, allowing these credentials to take the place of the smart card for remote authentication to federal systems. The publication describes how a user with a valid PIV card could obtain a derived credential on an integrated security token using either hardware or software cryptographic modules. This approach is in response to the mobile device authentication credential outlined in Federal Information Processing Standard (FIPS) 201-2*, Personal Identity Verification (PIV) of Federal Employees and Contractors*, published in August 2013.

NIST SP 800-157 does not address use of the PIV Card with mobile devices, but does provide an alternative in cases where using a PIV Card would be impractical. In lieu of the PIV Card, the alternative security token described in SP 800-157 can be implemented and deployed directly with mobile devices. The PIV credential associated with this alternative token is called a Derived PIV Credential. The use of a different type of token greatly improves the usability of electronic authentication from mobile devices to remote IT resources.

Introduction to Special Publication 800-157

The new Special Publication describes the life-cycle activities associated with derived PIV credentials, including aspects of issuance, usage, and maintenance. It describes the methods for adhering to Homeland Security Presidential Directive 12 (HSPD-12), including the requirement that the credential be established through an official accreditation process.

SP 800-157 Chapter 3 describes the technical requirements related to certificate policies, cryptographic specifications, and the security token types that may be used with mobile devices. It lists guidelines for cases in which the use of PIV Cards with mobile devices—using either contact card readers or Near Field Communication (NFC)—is deemed impractical. The guideline specifies the use of tokens with alternative form factors to the PIV Card that may either be inserted into mobile devices—such as Secure Digital (SD) cards, Universal Serial Bus (USB)

tokens, Universal Integrated Circuit Cards (UICC, the new generation of SIM cards)—or embedded in the mobile device. The embedded tokens may be either hardware or software cryptographic modules. The use of tokens with alternative form factors greatly improves the usability of electronic authentication from mobile devices to remote IT resources, while at the same time maintaining the goals of HSPD-12 for common identification that is secure, reliable, and interoperable governmentwide.

The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote systems. SP 800-157 also includes an informative annex that provides recommendations for the inclusion of digital signature and key management keys on mobile devices.

To achieve interoperability with the PIV infrastructure and its applications, public key infrastructure (PKI) technology has been selected as the basis for the Derived PIV Credential. Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63-2, *Electronic Authentication Guideline,* which leverages identity proofing and vetting results of current and valid credentials. When applied to PIV, identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential. Instead, the user that can demonstrate possession of a valid PIV Card may receive a Derived PIV Credential from their employer.

Cryptographic Token Types

The Derived PIV Credentials and their corresponding private keys may be used in a variety of cryptographic tokens available for use on mobile devices. These tokens may be hardware or software-only implementations.

Hardware tokens may either be removable or embedded within a mobile device. Three kinds of removable hardware tokens are permitted, each with well-defined physical and logical interfaces, to facilitate token portability between mobile devices in a manner analogous to PIV Card interchangeability:

- SD Card with Cryptographic Module
- Removable UICC with Cryptographic Module
- USB Token with Cryptographic Module

Embedded hardware tokens are not removable from the mobile device and may be accessed using the underlying interfaces of the device. However, these tokens are not intended to prohibit emulation of the PIV Card interface or removable token software interface. Similar rules apply to embedded software tokens.

Derived PIV Credentials in Relation to OMB Memoranda

NIST SP 800-157 provides a spectrum of choices for two-factor remote authentication with mobile devices, all of which are subject to Office of Management and Budget (OMB) guidance on remote electronic authentication.

The table below summarizes the association of Derived PIV Credentials' token types with the existing remote electronic authentication policies in OMB memoranda M-06-16 and M-07-16. At the time of this writing, both memoranda specify a "Control Remote Access" provision that calls for two-factor authentication where one of the two factors is provided by a device that is separate from the device accessing the remote resource.

Increasingly, mobile devices are becoming thinner and/or lighter. These constraints limit external ports and force the integration of authentication tokens and security features. As indicated by Column 6 in the table, four of the five tokens with Derived PIV Credentials are integrated. For these tokens, guidance will be updated by OMB to provide an alternative to current remote authentication policy. With integrated tokens, authentication factors are

not provided by a separate token; sensitive government information may be at greater risk of loss. OMB's alternative/updated guidance intends to address these risks by pointing to NIST guidelines for compensating controls (e.g., SP 800-53, SP 800-124, SP 800-164).

Credential Type	Token Type	PIV Assurance Level	Comparable OMB E-Authentication Level	Target Guidance:	
				Current M-06-16/M-07-16 for Separate Tokens	Alternate /Updated OMB Guidance for Integrated Tokens
Derived PIV Authentication certificate	MicroSD Token	Very High	4		✓
	USB Security Token	Very High	4	✓	
	Software Token	High	3		✓
	Embedded Hardware Token	Very High	4		✓
	UICC Token	Very High	4		✓
PIV Card's PIV Authentication certificate credential	PIV Card (via attached reader or NFC)	Very High	4	✓	

Table 1 - Token Types and Relation to OMB's Electronic Authentication Guidelines

Conclusion

SP 800-157 provides an identity verification alternative in cases where it would be impractical to use a PIV Card. An alternative security token can be implemented and deployed directly with mobile devices (such as smart phones and tablets). The use of such a different type of token allows users to enjoy the benefits of the unique capabilities of remote connectivity. Leveraging the derived PIV credentials facilitates more efficient and effective government while helping to ensure the confidentiality, integrity, and availability of information accessed by mobile devices.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov